UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A black Motorola Moto G Pure (XT2163DL), IMEI: 357852526271328, a SanDisk Ultra Plus 32GB SD card, Number: 2081YVDSE1MK found within the Motorola Moto G Pure, and a forensic extraction of data from those devices obtained by the New York State Police Forensic Investigation Center ("NYSP-FIC")

Case No. 5:23-mj-365 (ATB)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography

The application is based on these facts:
See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Martin H. Baranski
Applicant's signature

Martin H. Baranski, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: 6/28/2023

Andrew T. Baxter
Judge's signature

City and state: Syracuse, NY

Hon. Andrew T. Baxter, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, MARTIN H. BARANSKI, being duly sworn, deposes and states:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices and a forensic extraction of data—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B and/or a review of an extraction from that property of electronically stored information already obtained by the New York State Police, as described further below.

2. I am a Special Agent employed by the United States Department of Justice, Federal Bureau of Investigation (FBI), and as such I am an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Chapter 63. I have been a Special Agent with the FBI since October of 2018. I am currently assigned to the FBI's Albany Division where I investigate all federal criminal violations. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. I have received training in the area of child sexual exploitation and have had the opportunity to observe and review examples of child pornography in all forms of media including computer media.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: (A) a black Motorola Moto G Pure (XT2163DL), IMEI: 357852526271328, (B) a SanDisk Ultra Plus 32GB SD card, Number: 2081YVDSE1MK found within the Motorola Moto G Pure, and (C) a forensic extraction of data from those devices obtained by the New York State Police Forensic Investigation Center ("NYSP-FIC") pursuant to a request by the United States Probation Office for the Northern District of New York ("USPO") as part of its probation search authority. Items (A) and (B) are referred to together as "the Subject Devices." Items (A) through (C) are referred to collectively as the "Subject Devices and related forensic extraction."

5. The Subject Devices are currently located at the NYSP-FIC, 1220 Washington Avenue, Building 22, Albany, New York 12226. As described further below, there is probable cause to believe that a search of the Subject Devices and related forensic extraction will reveal evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt of child pornography) and (a)(5)(B) (possession of child pornography) (the "Subject Offenses").

6. The applied-for warrant would authorize the forensic examination of the Subject Devices and a review of the related forensic extraction for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On March 5, 2010, Steven Valder was sentenced by the Honorable David N. Hurd, U.S. District Judge in the Northern District of New York, to 120 months' imprisonment and a life term of supervised release following his conviction for Transportation of Child Pornography and Possession of Child Pornography. Valder began his term of supervised release on October 21, 2021.

8. Valder, a New York State designated level-three and high-risk sex offender due to a prior conviction in New York for Criminal Sexual Act 1st Degree: By Forcible Compulsion, also is on New York State parole.

9. On April 6, 2023, the USPO conducted a home visit at Valder's residence pursuant to its probation search authority and located multiple items that it considered contraband, including a drone and a laptop charger (despite Valder not having disclosed a laptop computer to the USPO as required if the device could access the internet).

10. On April 7, 2023, Valder failed a polygraph examination based on an examination question concerning whether he had used an electronic device to access the internet since his last polygraph. In the post polygraph examination interview, when Valder was confronted about his failure of the examination due to the question regarding accessing the internet, Valder argued with his probation officer that the test was broken and that he was being targeted. Valder would not directly answer whether he had accessed the internet and appeared to be redirecting to avoid discussing the issue.

11. On April 17, 2023, the USPO conducted a search of Valder's residence pursuant to its search authority but did not find any internet capable devices. The USPO questioned Valder about possessing an internet capable device, and he continued to deny any wrongdoing.

12. On May 17, 2023, the USPO located Valder outside of an address he had not reported to the USPO. A probation officer asked Valder if he consented to a search of his person, and he agreed. Valder emptied his pockets and was in possession of the Subject Devices. Valder said they belonged to the man he was with when the USPO arrived. The probation officer told Valder that he was in violation of his conditions of supervised release for possessing the Subject

Devices and that he should be truthful about the passcode. Valder has refused to provide the passcode.

13. On May 31, 2023, the Honorable David N. Hurd signed a warrant for Valder's arrest on a petition alleging several violations of the conditions of Valder's supervised release. *See* NDNY Dkt. 43 in 5:09-cr-260 (DNH). Valder had an initial appearance on that petition on June 1, 2023. *Id.* at Dkt. TEXT Minute Entry dated June 1, 2023. The Honorable Andrew T. Baxter ordered Valder detained pending the final revocation hearing, currently scheduled for July 12, 2023. *Id.* At Dkt. 49.

14. During a review of the Subject Devices before the related forensic extraction, and while the Subject Devices were still locked, the probation office was able to identify an email account. Although the cellular telephone was locked, the probation officer was able to see applications that appeared to be installed on the phone. While pressing and holding the email application, the phone displayed an email address. That email address contained a reference to low-rider bicycles, an item known to be a hobby/collectible for Valder. The email address also contained a zip code consistent with the zip code where Valder resided. The USPO provided the email account to the United States Marshal Service, and on May 30, 2023, the United States Marshal Service provided billing information from the email account that associated Valder to that account.

15. On June 13, 2023, the USPO sent the Subject Devices to the NYSP-FIC in Albany, New York, to perform a forensic extraction pursuant to the USPO's search authority.

16. On or about June 20, 2023, a forensically trained investigator from the NYSP-FIC informed the USPO that the NYSP-FIC obtained a forensic extraction of the Subject Devices. The NYSP-FIC began a review of that extraction and quickly observed what appeared to be child

pornography (*i.e.*, an image depicting the lewd and lascivious display of the genitals of prepubescent or early pubescent male).[1] The NYSP-FIC ceased its search at the direction of the FBI, in anticipation of the FBI seeking a search warrant for the Subject Devices and the related forensic extraction.

17. The Subject Devices are currently in storage at the NYSP-FIC, 1220 Washington Avenue, Building 22, Albany, New York 12226. In my training and experience, I know that the Subject Devices have been stored in a way that its contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the NYSP-FIC. Furthermore, it is the intent of the FBI to search the related forensic extraction as already obtained by the NYSP-FIC.

COLLECTORS OF CHILD PORNOGRAPHY

18. Based on my investigative experience I have learned that people who use the internet and mobile applications on cellular telephones to receive and possess child pornography often have a sexual interest in children and sexually explicit visual depictions of children. Such people commonly have the following characteristics and behaviors.

a. They receive sexual gratification, stimulation, and/or satisfaction from direct and indirect (*e.g.*, online) contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. They have a sexual interest in children or visual depictions of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines,

---

[1] A copy of this image is available to the Court upon request.

motion pictures, videos, books, slides and/or drawings. People who have a sexual interest in children or visual depictions of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to convince to engage in sexually explicit children, to arouse the selected child partner, and/or to demonstrate the desired sexual acts.

c. Likewise, people who have a sexual interest in children or visual depictions of children often maintain their collections in a digital or electronic format in a safe, secure, and private environment such a cell phone, laptop computer, desktop computer, external hard drive, and/or external storage media like flash drives and data cards. These collections (typically on an electronic device(s)) are often maintained for years and kept close by, usually at the person's residence, in his vehicle, on his person, or in online storage accounts that he controls. This type of access enables the individual to view the collection easily, which is valued highly.

d. People who have a sexual interest in children or visual depictions of children also often correspond with and/or meet other like-minded people to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors because they often find such interactions sexually arousing, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

e. In your affiant's training and experience, Valder displays characteristics common to people who receive and possess child pornography.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage

media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

22. Based on my knowledge training and experience, I also know that people who collect child pornography often use multiple devices to store and manage their collections. Additionally, digital evidence can be easily transferred from one device to another using various forms of electronic storage including CDs, DVDs, flash drives, and memory cards.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices and related forensic extraction because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain or exchange child pornography over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Devices consistent with the warrant and a review of the forensic extraction performed by NYSP-FIC. The

examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine devices and a related forensic extraction already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Devices and related forensic extraction described in Attachment A to seek the items described in Attachment B.

Attested to by the affiant:

Martin H. Baranski

Martin H. Baranski, Special Agent
Federal Bureau of Investigation

I, the Honorable Andrew T. Baxter, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on the 28th day of June 2023 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Andrew T. Baxter

Hon. Andrew T. Baxter
United States Magistrate Judge

ATTACHMENT A

The property to be searched is: (A) a black Motorola Moto G Pure (XT2163DL), IMEI: 357852526271328, (B) a SanDisk Ultra Plus 32GB SD card, Number: 2081YVDSE1MK found within the Motorola Moto G Pure, and (C) a forensic extraction of data from those devices obtained by the New York State Police Forensic Investigation Center ("NYSP-FIC"). Devices "A" and "B" are currently located at the NYSP-FIC, 1220 Washington Avenue, Building 22, Albany, New York 12226.

This warrant authorizes the forensic examination of the Devices "A" and "B" and a review of the forensic extraction of data from those devices obtained by the NYSP-FIC for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records constituting fruits, evidence, and/or instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(2)(A) (receipt of child pornography) and/or (a)(5)(B) (possession of child pornography):

a. Records concerning the receipt and/or possession of any visual depiction of a child engaged in sexually explicit conduct and evidence how any such depiction was received, including evidence of what device(s) was used to receive or possess the visual depiction and what application(s) was used to receive or possess the visual depiction and who was responsible for the receipt and/or possession of the depiction, including evidence of attribution for any device used to receive/possess such material;

b. Any visual depictions of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any visual depictions that might not meet the definition in the foregoing section but that might be considered child erotica;

c. Records evidencing intent, knowledge, and/or plan to receive and/or possess visual depictions of children engaged in sexually explicit conduct;

d. Records evidencing a sexual interest in children and/or child sexual abuse material such as visual depictions of children engaged in sexually explicit conduct, writings or drawings describing or depicting sexual activity involving children, or participation in chatrooms, social media groups, or private conversations concerning the sexual abuse of children and/or visual depictions of a children engaged in sexually explicit conduct.

e. Records concerning ownership and/or control of the devices identified in Attachment A;

f. Records of any passwords, passcodes, electronic keys, encryption codes, or any other electronic record for the purpose of using such record to gain access to all or part of the data on the devices authorized to be seized and searched pursuant to this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Photographs and Recordings of Search

During the search of the devices and forensic extraction identified in Attachment A, photographs and/or recordings may be taken to record the condition thereof and/or the location of items therein or thereon.